[Claims]

[Claim 1] An individual authentication method for authenticating a user's identification by extracting physical characteristics inherent in an individual person and using the physical characteristics, characterized by:

with authentication results in several kinds of physical characteristics stored in a table, selecting the most suitable physical characteristics for the authentication, of the several kinds of physical characteristics, by calculating an estimation function indicating a reliability of each kind of physical characteristics using information on a predetermined security level of the individual authentication and the information of the table; requesting a user to enter the corresponding physical characteristics; and comparing the physical characteristics obtained from the user with the previously-registered physical characteristics of a specified individual person, so to judge whether the above physical characteristics belong to the specified individual person or not; when it is judged that the above physical characteristics belong to the specified individual person, finishing the authentication processing, while when it is not judged, performing the authentication by using a next candidate for the physical characteristics from the estimation function, in a way of repeating step-by-step selection of the physical characteristics until using all several kinds of physical characteristics.

[Claim 2] An individual authentication method for authenticating a user's identification by extracting physical

characteristics inherent in an individual person and using the physical characteristics, in which a user terminal is connected to a center system through a communication network and the center system or a user selects one kind of physical characteristics to use for authentication, one by one, of several kinds of physical characteristics, the method characterized in that when the center system selects physical characteristics, with authentication results of the several kinds of physical characteristics stored in a table, the center system selects the most suitable physical characteristics for the authentication, of the several kinds of physical characteristics, by calculating an estimation function indicating a reliability of each kind of physical characteristics by using information on a predetermined security level of the individual authentication and the information of the above table, and transmits a name of the above physical characteristics to the user terminal; the user enters the physical characteristics specified by the center system, extracts the physical characteristics, and transmits the above to the center system; the center system compares the physical characteristics transmitted from the user terminal with the previously-registered physical characteristics of the specified individual person, so to judge whether the above physical characteristics belong to the above specified individual person or not, when it is judged that the above characteristics belong to the specified individual person, the center system finishes the authentication processing, while when it is not judged, it performs the authentication by using a next

candidate for the physical characteristics according to the selection, step by step, repeatedly until using all the several kinds of physical characteristics; while when the user selects physical characteristics, the user enters the own specified physical information, extracts the physical characteristics, and transmits the same to the center system; the center system compares the physical characteristics transmitted from the user terminal with the previously-registered physical characteristics of the specified individual person, so to judge whether the above physical characteristics belong to the specified individual person or not, when it is judged that the above characteristics belong to the specified individual person, the center system finishes the authentication processing, while when it is not judged, it performs the authentication by using a next candidate for the physical characteristics according to the specification, step by step, repeatedly until using all the several kinds of physical characteristics.

[Claim 3] An individual authentication method for authenticating a user's identification by extracting physical characteristics inherent in an individual person and using the physical characteristics, in which a user terminal is connected to a center system through a communication network, the center system or a user selects the physical characteristics to use for authentication, one by one, of several kinds of the physical characteristics, and the processing concerned with the authentication is divided into two of preprocess and post-process, the method characterized in that when the center system selects

physical characteristics, with authentication results of the several kinds of physical characteristics stored in a table, the center system transmits the most suitable physical characteristics for the authentication, of the several kinds of physical characteristics, by calculating an estimation function indicating a reliability of each kind of physical characteristics by using information on a predetermined security level of the individual authentication and information of the table and a processing method of the preprocess to the terminal; the terminal enters the physical characteristics specified by the center system according to the preprocessing, extracts the physical characteristics, and transmits the above to the center system; the center system compares the physical characteristics transmitted from the terminal with the previously-registered physical characteristics of the specified individual person according to the post-processing, so to judge whether the above physical characteristics belong to the specified individual person or not, when it is judged that the above characteristics belong to the specified individual person, the center system finishes the authentication processing, while when it is not judged, it performs the authentication by using a next candidate for the physical characteristics according to the selection, step by step, repeatedly until using all the several kinds of physical characteristics; while when the user selects physical characteristics to use, the user terminal enters the physical information specified by the user according to the preprocessing method transmitted from the authentication server, extracts the

physical characteristics, and transmits the same to the center system; the center system compares the physical characteristics transmitted form the terminal with the previously-registered physical characteristics of the specified individual person according to the post-processing, so to judge whether the above physical characteristics belong to the specified individual person or not, when it is judged that the above physical characteristics belong to the specified individual person, the center system finishes the authentication processing, while when it is not judged, it performs the authentication by using a next candidate for the physical characteristics according to the specification, step by step, repeatedly until using all the several kinds of physical characteristics.

[Claim 4] The individual authentication method according to Claim 2 or Claim 3, characterized in that a communication between the center system and the user terminal is performed by a public key coding method.

[Claim 5] The individual authentication method according to one of Claims 1 to 3, characterized in that contents of the table are updated according to judgment results obtained in every authentication.

[Claim 6] A storing medium of storing an individual authentication program for making a computer execute processing for authentication by using one of several kinds of physical characteristics, characterized by comprising

a procedure of storing authentication results into a table, a procedure for setting a security level of individual

authentication, a procedure of selecting the most suitable physical characteristics for authentication, of the several kinds of physical characteristics, by calculating an estimation function indicating a reliability of each kind of physical characteristics using information of the security level and information of the table, and a procedure of comparing the physical characteristics obtained from a user with the previously-registered physical characteristics of a specified individual person, so to judge whether the above physical characteristics belong to the specified individual person or not; when it is judged that the above physical characteristics belong to the specified individual person, finishing the authentication processing, while when it is not judged, performing the authentication by using a next candidate for the physical characteristics from the above estimation function, step by step, repeatedly until using all the several kinds of physical characteristics.

[Claim 7] The storing medium of storing the individual authentication program according to Claim 6, characterized in that contents of the table are updated according to judgment results obtained in every authentication.

[Claim 8] A storing medium which stores an individual authentication program for performing processing of a center system for authentication by a center system's or a user's selecting physical characteristics to use, one by one, of several kinds of physical characteristics, with a user terminal connected to the center system through a communication network,

characterized by comprising a procedure of storing authentication results of the several kinds of physical characteristics into a table, a procedure of setting a security level of individual authentication, a procedure of selecting the most suitable physical characteristics for authentication, of the several kinds of physical characteristics, by calculating an estimation function indicating a reliability of each kind of physical characteristics using information of the security level and information of the table, and a procedure of comparing the physical characteristics transmitted from the user terminal with the previously-registered physical characteristics of a specified individual person, so to judge whether the above physical characteristics belong to the specified individual person or not; when it is judged that the above physical characteristics belong to the specified individual person, finishing the authentication processing, while when it is not judged, performing the authentication by using a next candidate for the physical characteristics from the above estimation function, step by step, repeatedly until using all the several kinds of physical characteristics.

[Claim 9] A storing medium of storing an individual authentication program for performing processing of a user terminal for authentication by a center terminal's or a user's selecting physical characteristics to use, one by one, of several kinds of physical characteristics, with a user terminal connected to the center system through a communication network, characterized by comprising a procedure of setting a security

level of individual authentication by the user itself, a procedure of entering the specified physical information, extracting the physical characteristics, and transmitting the above to the center system, and a procedure of repeating step-by-step selection such as authenticating the user by using a next candidate for the physical characteristics according to the specification when the user is not authenticated in the center system, until using all the several kinds of physical characteristics.

[0003]

[Problems to be Solved by the Invention]

The use method of several items of biometric information is roughly divided in the following two types. At first, the authenticating means is doubled and as shown in Japanese Patent Publication No. 10-137222, when a user is not authenticated by using one of the two kinds of biometric information, a method of performing the authentication by using the other is used, hence to prevent from a wrong rejection in the case of the identified user. At second, the authentication accuracy is improved, and as shown in Japanese Patent Publication No. 08-16788 and No. 10-137221, a weighting connection of the authentication results of several items of biometric information is often used. In the first method, however, the user acceptance becomes easy but a function of rejection of the other person is deteriorated, and in the second method, since the weight is fixed, it has the problem that the weight cannot be adjusted when there occurs

a request different from at a time of designing the system or when there occurs a change in the using environment.

[0004]

As mentioned above, according to the conventional methods, there is such a problem that how to use several kinds of biometric information is not determined in such circumstances that the priority of the user acceptance and the rejection of the other person differs depending on the purpose of its use. Further, it is necessary to customize the authentication method individually in order to configure an authentication server depending on various purposes of use and further tune it delicately in order to cope with a change in the environment, which is troublesome disadvantageously. The invention is to solve the above problems and its object is to provide an individual authentication method and its system capable of satisfying the both requests of the user acceptance/rejection of the other person and further to provide an individual authentication method and its system highly adaptable according to the real using environment.

[0013]

[Mode for Carrying Out the Invention]

This time, an embodiment of the present invention will be described with reference to the drawings. Fig. 1 is a block diagram of an individual authentication system showing one embodiment of the invention, which comprises a user 1, a user terminal 2, a communication network 3, and an authentication

server 4. The authentication server can be referred to as a center system. The user terminal 2 comprises an input unit 21, a preprocessor 22, a display 23, and a using order memory 24, and the preprocessor 22 includes N pairs of different sensors (sensor 1 (221), sensor 2 (222), ···, sensor N (223)) and corresponding characteristic extracting units (characteristic extracting unit 1 (224), characteristic extracting unit 2 (225), ···, characteristic extracting unit N (226)). The authentication server 4 includes a priority setting unit 41, a table for storing judgment results 42, a selecting unit 43, a postprocessor 44, and a personal characteristic memory 45. The postprocessor 44 includes N pairs of matching units (matching unit 1 (441), matching unit 2 (442), ···, matching unit N (443)) and corresponding judging units (judging unit 1 (444), judging unit 2 (445), ···, judging unit N (446)).

[0014]

According to this individual authentication system, the user terminal 2 obtains the physical characteristics, according to the information obtained by one of the several sensors, from the characteristic extracting unit corresponding to the sensor, and the authentication server 4 compares the physical characteristics with the registered characteristics, hence to authenticate the identification. The operation of this embodiment will be described by using the processing flow of Fig. 2. In the flow of Fig. 2, especially, a notice is taken into the processing of selecting one from several items of biometric information and using the same.

[0015]

In Step 501, it is possible to select whether the right of selecting which item of biometric information is used, of the several items of biometric information, belongs to the authentication server 4 or the user 1. This can be selected by, for example, a user. When the selection right belongs to the authentication server 4, the authentication server 4 determines the using order k (k=1, 2, ···, N) of the items of biometric information. When k=1 is set (Step 502), the authentication server 4 transmits a message instructing a user to enter the k-th item of biometric information, to the display 23 through the communication network 3. The user 1 enters the k-th item of biometric information from the specified sensor of the number N according to the instruction on the display 23. The user terminal 2 transmits the extracted characteristics to the authentication server 4 through the communication network 3 and the authentication server 4 performs the authentication in the postprocessor 44 (Step 503). When the user 1 is authenticated (Step 504), a message informing the user of the acceptance is shown on the display 23 (Step 505) and the processing is finished.

[0016]

When the user is not authenticated (Step 504), k is set at k=k+1 (Step 506), authentication is performed (Step 503) by using the item of biometric information specified next, of the biometric information items which have not bee used yet in k times of authentication, and the user's identification is judged

(step 504). When the above processing is repeated, so to use the whole specified N items of biometric information (k>N), and as a result, when the user is not authenticated yet (Step 507), the operation will be retried at the beginning (Step 508).

[0017]

When the selection right belongs to the user 1, the user 1 sets the using order k of the biometric information items with the input unit 21 (Step 509). The user terminal 2 is set at k=1 (Step 510), and authentication by using the k-th item of biometric information is performed (Step 511). When the identification of the user 1 is authenticated (Step 512), the operation is accepted (Step 513), and the processing is finished. When the user's identification is not authenticated (Step 512), k is updated to k=k+1 (Step 514), and authentication is repeated by changing the items of biometric information to use. Even if using all the N items of biometric information specified (k>N), when the user's identification is not authenticated (Step 515), the operation will be retried again at the beginning (Step 516).

[0018]

This time, the detailed operation of this embodiment will be described by using Fig. 3 and Fig. 4. Fig. 3 is a view showing the processing flow in the case where the selection right belongs to the authentication server 4. When the user 1 enters the ID number with the input unit 21, it is transmitted to the authentication server 4 (Steps 1 and 2). There is a wide variety of the biometric information items including that one having the high authentication accuracy or the low authentication

accuracy and the user friendly information or the user inconvenient information. The item of biometric information is selected by the processing in the priority setting unit 41, the judgment result storing table 42, and the selecting unit 43. Here, the outline is described and the details will be described later.

[0019]

The priority setting unit 41 calculates the security level required by the above status and service and determines the degree of the respective elements of user acceptance and rejection of the other person (Step 3). The selecting unit 43 determines the first item of biometric information to use at first, from the N items of biometric information (Steps 4 and 5), in the following method, according to the degree of the user acceptance and the rejection of the other person and the contents of the judgment result storing table 42 having the previous authentication results of the user 1 by using respective items of biometric information, and transmits its name to the user terminal 2 and displays it on the display 23 (Step 6).

[0020]

The user 1 enters the same biometric information by using the sensor corresponding to the first item of biometric information shown on the display (Step 7), extracts the characteristics by executing a program existing in the preprocessor 22 (Step 8), and transmits the same to the authentication server 4. The authentication server 4 receives the characteristics (Step 9), activates a program of the matching

unit corresponding to the first item of biometric information, so to compare the registered characteristics of the user 1 stored in the personal characteristic memory 45 with the transmitted characteristics of the first item of biometric information and obtain the scale of similarity or difference (Step 10). The judging unit checks whether the above characteristics of the first item of biometric information really belongs to the identical user, by using the threshold for the above scale, writes the judgment result into the judgment result storing table 42, and updates the contents thereof. When the judgment result really belongs to the identical user, log-in to the user terminal 2 is accepted (Steps 11, 12), when it belongs to the other person, it is rejected (Step 13). When there occurs the rejection, the selecting unit 43 determines the second item of biometric information to use at second, from the remaining (N-1) items of biometric information and transmits its name to the user terminal 2, thereby performing the authentication according to the second item of biometric information through the above processing (Step 14 and the later). Hereinafter, the above processing will be repeated until the user's identification is authenticated, and when it is not authenticated even if using all the items of biometric information, the operation will be retried again at the beginning.

[0021]

Fig. 4 shows the processing in the case where the selection right belongs to the user 1. The user 1 enters the ID number (Step 1) and sequentially specifies the convenient items of

biometric information from the viewpoint of efficiency and user-friendly operation, enabling the user to be accepted at high accuracy, and then the contents thereof are stored in the using order memory 24 (Steps 2 and 3). Successively, the contents of the using order memory 24 are read out and a message to the effect of inducing the user to enter the first item of biometric information appears on the display 23, when the user 1 enters the biometric information by using the sensor corresponding to the first item of biometric information, executes the program existing in the preprocessor 22, to extract the characteristics, and transmits the same to the authentication server 4 (Steps 4 and 5).

[0022]

Hereinafter, the processing from the matching/judgment to the user acceptance or rejection is the same as the processing in Fig. 3. It is the post-processing in the case of rejection that is different from the above; in Fig. 3, the authentication server 4 transmits the name of the biometric information decided to be used at second to the user terminal 2, while in Fig. 4, it transmits a notice of the user rejection there (Step 9). When the user terminal 2 receives the notice of the user rejection (Step 10), the user 1 performs the authentication by using the second item of biometric information in the same processing as mentioned above, the above processing will be repeated until the user identification is authenticated (Step 11 and the later), and when it is not authenticated even if using all the items of biometric information, the operation will be retried again

at the beginning.

[0023]

Next, the above processing of selecting the biometric item will be described in detail. Fig. 5 is a view showing the contents of the judgment result storing table 42, where the number T of using times and the number R of the times of user rejections and the number A of acceptance times of the other person are stored for every item of biometric information. The above T, R, and A are all set at the initial value of zero. When the authentication is performed by using some item of biometric information, T corresponding to the item is incremented by 1, and as a result of the authentication, when the user 1 is not authenticated, R is incremented by 1. Since it is difficult to measure the number A of acceptance times of the other person in the actual operation, when the user 1 is not authenticated, all the characteristics of the users other than the user 1, stored in the personal characteristic memory 45, are regarded as an input, and when the input is compared with the characteristics of the user 1 and accepted as the user 1, A is incremented by 1 assuming that the acceptance of the other person has been performed. Thus, the values of T, R, and A are updated every time of authentication.

[0024]

Fig. 6 is a constitutional view of the selecting unit 43, comprising an estimation function calculating unit 431 and a maximum value detecting unit 432. The estimation function calculating unit 431 requires the value of an estimation function

G of the expression (1) by using the importance α of the acceptance of the other person in the user rejection entered from the priority setting unit 41 and the using times T, the user rejection times R, the acceptance times A of the other person entered from the judgment result storing table 42.

$$G=1-(R+\alpha A)/T \qquad \cdots (1)$$

In the second term of the right side of the expression (1), A is multiplied by the weight α, in comparison with R. The second term of the right side of the expression (1) is the term for penalty, the value of G is more increased according as the values of A and R become smaller and when R=A=0, it takes the maximum value 1. The maximum value detecting circuit 432 detects the maximum value of the G of the target, displays the item name of the corresponding biometric information on the display 23 of the user terminal 2, and induces the user 1 to enter the same biometric information. Since the G is calculated every time of authentication, when the authentication accuracy of the biometric information of the user 1 which has been frequently used at first falls down with elapse of time, the authentication server 4 finds the alternative item of biometric information. Even when there is a user having the biometric information similar to the biometric information of the user 1, of many users, since the authentication server 4 is designed to use the different biometric item from the above, authentication of high reliability is possible. When a new user having the similar biometric

information takes part in the system halfway, it is possible to switch the above biometric information item to the different one according to the induction of the authentication server 4. As mentioned above, even when there is a change in the using environment, since the system is designed to follow the change, stable authentication is always possible. Further, since the above operation is automatically performed by the authentication server 4, it is not necessary to customize and tune the system by man power.

[0025]

Fig. 3 and Fig. 4 respectively show the procedure in the case where the programs of the preprocessing and the post-processing are respectively set in the preprocessor 22 and the postprocessor 44, and the program of the preprocessing, however, can be transmitted by the authentication server 4 and Fig. 7 and Fig. 8 show the procedure in this structure. Here, the ProGUI and the like used for the following description is the symbol indicating each component and hereinafter, the component may be referred to only by the symbol in some cases.

[0026]

Fig. 7 shows the processing in the case where the selection right belongs to the authentication server 4. The user 1 creates a public key Pk(A) and a secret key Sk(A) of a user and transmits the Pk(A) and the ID number to the authentication server 4 (Steps 1 and 2). The authentication server 4 receives them (Step 3) and sequentially activates the priority setting unit 41 and the selecting unit 43 (Steps 4 and 5), and obtains the first item

of biometric information B1 (Step 6). Further, it reads out the GUI control program ProGUI for displaying the input menu of the biometric information on the user terminal 2 (Step 7). Further, the authentication server 4 gets the EPk(A) (ProFow, SXPro) (Step 8) by encrypting the characteristic extraction program ProFow and the scramble program SXPro by Pk(A), and transmits the B1, ProGUI, EPk(A) (ProFow, SXPro) to the user terminal 2. In the user terminal 2, the ProFow and the SXPro are decoded with the secret key Sk(A) (Steps 9 and 10), the user 1 enters the information from the sensor corresponding to the B1 according to the instruction of the ProGUI (Step 11) to extract the characteristics Kaz by executing the ProFow (Step 12). Next, the Kaz is scrambled by the SXPro to get Kaz(-1) (Step 13), and transmits ESk(A)(Kaz(-1), ID) obtained by encrypting the above by ESk(A), to the authentication server 4 (Step 14).

[0027]

The authentication server 4 decodes the above by PK(A) (Steps 15 and 16), so to take out the Kaz(-1). The scrambled characteristics Kaz[0](-1) of the user 1 are read out from the personal characteristic memory 45 (Step 17), and the Kaz and Kaz[0] are decoded by the scramble decoding program SXPro(-1) (Step 18). Thereafter, a series of the processing of activating the matching unit and the judging unit for authentication is the same as that in Fig. 3.

[0028]

Fig. 8 shows the processing in the case where the selection right belongs to the user 1. The user 1 sequentially specifies

the convenient items of biometric information from the viewpoint of efficiency and user-friendly operation, enabling the user to be accepted at high accuracy, and stores the above in the using order memory 24. The user 1 transmits the public key Pk(A) and the ID number of the user and the B1 read from the using order memory 24 to the authentication server 4 (Steps 1 to 3), extracts the characteristics Kaz by using the characteristic extraction program ProFow of the B1 returned from the authentication server 4 (Steps 4 to 9), and transmits the data scrambled by the scramble program SXPro and the name of the first item B1 read from the using order memory 24, to the authentication server 4 (Steps 10 and 11).

[0029]

Thereafter, the processing of the matching/judgment and the user acceptance/rejection is the same as the processing of Fig. 7. It is the post-processing in the case of rejection that is different from the above; in Fig. 7, the authentication server 4 transmits the program ProGUI and ProFow for extracting the B2 and the characteristics of the B2 and the scramble program SXPro to the user terminal 2, while in Fig. 8, the B2 is not necessary in Fig. 8. When receiving the above data, the user 1 performs the authentication by using the B2 in the same processing as mentioned above, and hereinafter, the above processing is repeated until the user identification is authenticated, and when it is not authenticated even if using all the items of biometric information, the operation will be retried again at the beginning.

[0030]

As mentioned above, by dividing the process in the individual authentication processing, into the respective processing in the terminal and the server, security can be kept and the communication amount can be reduced. By encrypting the program and transmitting the same program to the terminal, it is possible to change the algorithm easily and further enhance the security.

[0031]

The individual authentication system of the invention is not restricted to the above structure shown in Fig. 1, but various structures are possible. For example, it may be formed in the structure shown in Fig. 9. This individual authentication system comprises the user 1, the user terminal 2, the communication network 3, and the authentication server 4. In Fig. 1, the matching units (the matching unit 1 (441), the matching unit 2 (442), ···, the matching unit N (443)) are provided in the authentication server 4, while in Fig. 9, they are provided in the user terminal 2 differently.

[0032]

In this example, the selection right of selecting which item to use, of several items of biometric information, may belong to the authentication server 4 or the user 1. When the selection right belongs to the authentication server 4, the authentication server 4 sets the using order k of the items of the biometric information (k=1, 2, ···, K, K; the number of the items of biometric information to use). When k=1 is set, the authentication server

4 instructs the display 23 to show the effect of asking a user to enter the biometric information through the communication network 3. The user 1 enters the k-th item of biometric information from the specified sensor, of the N sensors, to check the matching by using the extracted characteristics, transmits the result to the authentication server 4 through the communication network 3, and the authentication server 4 checks the user's identification in the judging unit. When the user 1 is authenticated, a message indicating the acceptance appears on the display 23 and the processing is finished. When the user is not authenticated, k is set at k=k+1, and the authentication is performed in the above procedure by using the biometric information of the item specified next. The above processing is repeated, and when the user is not authenticated even if using all the specified N items of biometric information, the operation will be retried again at the beginning.

[0033]

When the selection right belongs to the user 1, the user 1 sets the using order k of the items of biometric information with the input unit 21 and stores the above into the using order memory 24. The user terminal 2 sets the order at k=1 and performs the authentication by using the k-th item of biometric information. When the user 1 is authenticated, the operation is accepted and the processing is finished. When it is not authenticated, k is updated to k=k+1, and the information stored in the using order memory 24 is read out, and the authentication is repeated by changing the items of biometric information to

use. Even when using all the specified N items of biometric information, when the user's identification is not authenticated, the operation will be retried again at the beginning.

[0034]

In this embodiment of Fig. 9, although the matching units (the matching unit 1 (441), the matching unit 2 (442), ···, the matching unit N (443)) are provided in the user terminal 2, also the judging units (the judging unit 1 (444), the judging unit 2 (445), ···, the judging unit N (446)) may be provided in the user terminal 2 and only the judgment result may be transmitted to the authentication server 4. Alternatively, the individual authentication system may be formed in a standalone system which can perform all the characteristic input, the judgment, and the selection of the biometric information item.

[0035]

A program for realizing the above-mentioned respective components can be stored in a storing medium such as a CD-ROM, a floppy disk (registered mark), and the like. The processing of the terminal and the authentication server of the invention can be performed by installing the program stored in the storing medium into a computer. Alternatively, the above program may be pre-installed into a computer.

[0036]

As mentioned above, although the invention has been concretely described based on the embodiment, the invention is not restricted to the embodiment, but it is needless to say that it can be variously modified without departing from its sprit.

[0037]

[Advantage of the Invention]

As described above, according to the invention, since the priority setting of the user acceptance/rejection of the other person is performed by the user or the authentication server and the authentication result of the biometric information in the operation process is registered in the table as the statistic information and updated every time of authentication, it has the advantage of using the optimum item of biometric information while keeping the specified priority. Since it is designed to update the information automatically, it has the advantage of decreasing the trouble in applying this system to various kinds of uses and the advantage of applying this system to the changing circumstances with elapse of time.

Fig. 1

1: block diagram of individual authentication system indicating one embodiment of the invention

1: user

2: user terminal

3: communication network

4: authentication server

21: input unit

22: preprocessor

23: display

24: using order memory

41: priority setting unit

42: judgment result storing table

43: selecting unit

44: postprocessor

45: personal characteristic memory

221: sensor 1

222: sensor 2

223: sensor N

224: characteristic extracting unit 1

225: characteristic extracting unit 2

226: characteristic extracting unit N

441: matching unit 1

442: matching unit 2

443: matching unit N

444: judging unit 1

445: judging unit 2

446: judging unit N

Fig. 2

1: flow chart of the processing of the individual authentication system in Fig. 1

S501: the selection right of using biometric item belongs to which? user authentication server

S503: authentication by using the k-th item of biometric information specified by the authentication server

S504: the identified user?

S505: displaying "acceptance"

S508: displaying "retry"

S509: entering the order k of the biometric information to use (k=1, 2, ···, N)

S511: authenticated by using the k-th item of biometric information specified by a user

S512: the identified user?

S513: displaying "acceptance"

S516: displaying "retry"

Fig. 3

0: flow chart of communication control in the case where the selection right belongs to the authentication server 4 in the individual authentication system in Fig. 1

1: ID input

2: receiving ID

3: activating the priority setting unit

4: activating the selecting unit

5: determining the first biometric information

6: receiving the name of the first biometric information

7: entering the first biometric information

8: extracting the characteristics of the first biometric information

9: receiving the characteristics of the first biometric information

10: activating the matching unit

11: user acceptance

12: finishing

13: user rejection

14: activating the selecting unit

15: reading out the second biometric information

16: receiving the name of the second biometric information

17: hereinafter, repeating (7) and (8)

18: ID

19: the name of the first biometric information

20: first biometric characteristics

21: the name of the second biometric information

Fig. 4

0: flow chart of communication control in the case where the selection right belongs to the user 1 in the individual authentication system in Fig. 1

1: ID input

2: setting the biometric information to use

3: entering the first biometric information

4: extracting the characteristic of the first biometric information

5: receiving the characteristics of the first biometric information

6: activating the matching unit

7: user acceptance

8: finishing

9: user rejection

10: receiving a notice of the user rejection

11: reading out the second biometric information

12: hereinafter, repeating (3) and (4)

13: user terminal

14: authentication server

15: first biometric characteristics

16: notice of user rejection

Fig. 5

1: view showing one example of the judgment result storing table 42

2: using times

3: user rejection times

4: acceptance times of the other person

5: biometric information 1

biometric information 2

biometric information N

Fig. 6

1: block diagram of the selecting unit 43

2: judgment result storing table 42

3: priority setting unit 41

4: selecting unit

5: estimation function calculating unit

6: maximum value detecting unit

7: selection result

8: communication network

Fig. 7

0: flow chart of communication control in the case where the selection right belongs to the authentication server 4 and the program of the preprocessing is transmitted from the authentication server 4 in the individual authentication system in Fig. 1

1: creating the public key Pk(A) and the secret key Sk(A) of a user

2: ID input

3: receiving the Pk(A) and ID

4: activating the priority setting unit

5: activating the selecting unit

6: determining the first biometric information B1

7: reading out the GUI control program ProGUI

8: creating EPk(A)(ProFow, SXPro) by encrypting the characteristic extraction program ProFow and the scramble program SXPro by Pk(A)

9: receiving B1, ProGUI, EPk(A)(ProFow, SXPro)

10: decoding ProFow and SXPro by Sk(A)

11: entering Bi according to the instruction of ProGUI

12: extracting the characteristics Kaz of B1 by using ProFow

13: obtaining Kaz(-1) by scrambling Kaz by SXPro

14: creating ESk(A)(Kaz(-1), ID) by encrypting Kaz(-1) by Sk(A)

15: receiving ESk(A)(Kaz(-1), ID)

16: decoding Kaz(-1) by Pk(A)

17: reading out the registered characteristics Kaz[0](-1) scrambled

18: decoding Kaz, Kaz[0] by the scramble decoding program SXPro(-1)

19: activating the matching unit

20: user acceptance

21: finishing

22: user rejection

23: activating the selecting unit

24: reading out the second biometric information B2

25: receiving B1, ProGUI, EPk(A)(ProFow, SXPro)

26: hereinafter, repeating (9) and (14)

25: user terminal

26: authentication server

Fig. 8

0: flow chart of communication control in the case where the selection right belongs to the user 1 and the program of the preprocessing is transmitted from the authentication server 4

in the individual authentication system in Fig. 1

1: setting the biometric information to use

2: creating the public key Pk(A) and the secret key Sk(A) of a user

3: ID input

3: receiving Pk(A), ID, and B1

4: reading out the GUI control program ProGUI

5: creating EPk(A)(ProFow, SXPro) by encrypting the characteristic extraction public program ProFow and the scramble program SXPro by Pk(A)

6: receiving ProGUI and EPk(A)(ProFow, SXPro)

7: decoding ProFow and SXPro by Sk(A)

8: entering B1 according to the instruction of ProGUI

10: obtaining Kaz(-1) by scrambling Kaz by SXPro

11: creating ESk(A)(Kaz(-1), ID) by encrypting Kaz(-1) by Sk(A)

12: receiving ESk(A)(Kaz(-1), ID)

13: decoding Kaz(-1) by Pk(A)

14: reading out the registered characteristics Kaz[0](-1) scrambled

15: decoding Kaz[0] by the scramble decoding program SXPro(-1)

16: activating the matching unit

17: user acceptance

18: finishing

19: user rejection

20: receiving ProGUI, EPk(A)(ProFow, SXPro)

21: reading out the second biometric information B2

22: hereinafter, repeating (6) and (11)

20: user terminal

21: authentication server

Fig. 9

0: block diagram of the individual authentication system indicating another embodiment of the invention

1: user

2: user terminal

3: communication network

4: authentication server

21: input unit

22: preprocessor

23: display

24: using order memory

41: priority setting unit

42: judgment result storing table

43: selecting unit

45: personal characteristic memory

221: sensor 1

222: sensor 2

223: sensor N

224: characteristic extracting unit 1

225: characteristic extracting unit 2

226: characteristic extracting unit N

441: matching unit 1

442: matching unit 2

443: matching unit N

```
444: judging unit 1
445: judging unit 2
446: judging unit N
```

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2001－52181
(P2001－52181A)
(43)公開日　平成13年２月23日(2001.2.23)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'(参考)
Ｇ０６Ｔ　7/00		Ｇ０６Ｆ　15/62	４６５Ａ	５Ｂ０４３
Ｇ０６Ｆ　1/00	３７０	1/00	３７０Ｅ	５Ｂ０８５
15/00	３３０	15/00	３３０Ｆ	

審査請求　未請求　請求項の数９　ＯＬ　（全 17 頁）

(21)出願番号　特願平11－229457

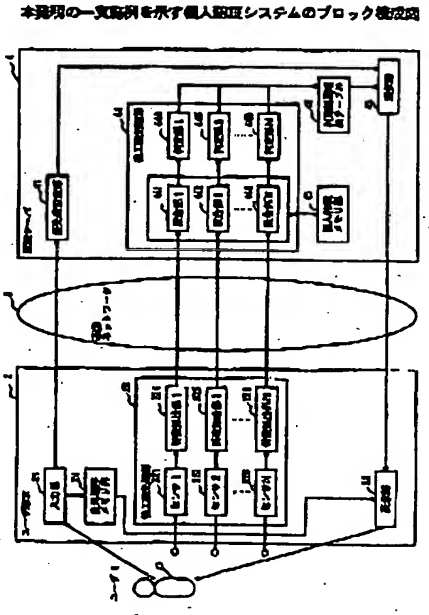
(22)出願日　平成11年８月13日(1999.8.13)

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(72)発明者　木村　義政
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　伴野　明
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(74)代理人　100070150
弁理士　伊東　忠彦

最終頁に続く

(54)【発明の名称】　個人認証方法及び個人認証プログラムを記録した記録媒体

(57)【要約】
【課題】　本人受理・他人拒否の両要求を満足する個人認証方法を提供し、また、実際の使用環境に追随して適応していく個人認証方法を提供する。
【解決手段】　複数種類の身体的特徴における認証結果をテーブルに記憶しておき、予め設定された個人認証のセキュリティレベルの情報と前記テーブルの情報とを用いて各身体的特徴の信頼性を表わす評価関数を計算することにより前記複数種類の身体的特徴の中から認証に最も適する身体的特徴を選定して利用者に該身体的特徴の入力を要求し、利用者から得られた身体的特徴と予め登録している特定個人の身体的特徴とを照合し判定を行い、前記特定個人と判定されたときは認証処理を終了し、前記特定個人と判定されなかったときは前記評価関数により次候補として挙げられた身体的特徴を用いて認証するという段階的選定を複数種類の身体的特徴を全て使用するまで反復して行う。



【特許請求の範囲】

【請求項１】 個人固有の身体的特徴を抽出し該身体的特徴を用いて本人確認を行う個人認証方法において、

複数種類の身体的特徴における認証結果をテーブルに記憶しておき、予め設定された個人認証のセキュリティレベルの情報と前記テーブルの情報とを用いて各身体的特徴の信頼性を表わす評価関数を計算することにより前記複数種類の身体的特徴のなかから認証に最も適する身体的特徴を選定して利用者に該身体的特徴の入力を要求し、利用者から得られた身体的特徴と予め登録している特定個人の身体的特徴とを照合し前記身体的特徴が前記特定個人のものか否かの判定を行い、前記特定個人と判定されたときは認証処理を終了し、前記特定個人と判定されなかったときは前記評価関数により次候補として挙げられた身体的特徴を用いて認証するという段階的選定を複数種類の身体的特徴を全て使用するまで反復して行うことを特徴とする個人認証方法。

【請求項２】 個人固有の身体的特徴を抽出し該身体的特徴を用いて本人確認を行う個人認証方法において、利用者側端末が通信ネットワークを介してセンタ側装置に接続されており、前記センタ側装置あるいは利用者が複数種類の身体的特徴のなかから使用する身体的特徴を順に選定して認証に用いる方法であって、

センタ側装置が身体的特徴の選定を行う場合には、複数種類の身体的特徴における認証結果をテーブルに記憶しておき、予め設定された個人認証のセキュリティレベルの情報と前記テーブルの情報とを用いて各身体的特徴の信頼性を表わす評価関数を計算することにより複数種類の身体的特徴のなかから認証に最も適する身体的特徴を選択して該身体的特徴の名称を前記利用者側端末に送信し、利用者は前記センタ側装置が指定した身体的情報を入力して身体的特徴の抽出を行い前記センタ側装置に送信し、前記センタ側装置では前記利用者側端末から送信された身体的特徴と予め登録している特定個人の身体的特徴とを照合し前記身体的特徴が前記特定個人のものか否かの判定を行い、前記特定個人と判定されたときは認証処理を終了し、前記特定個人と判定されなかったときは前記選択により次候補として挙げられた身体的特徴を用いて認証するという段階的選定を前記複数種類の身体的特徴を全て使用するまで反復して行い、利用者が身体的特徴の選定を行う場合には、利用者は自ら指定した身体的情報を入力して身体的特徴の抽出を行い前記センタ側装置に送信し、前記センタ側装置では前記利用者側端末から送信された身体的特徴と予め登録している特定個人の身体的特徴とを照合し前記身体的特徴が前記特定個人のものか否かの判定を行い、前記特定個人と判定されたときは認証処理を終了し、前記特定個人と判定されなかったときは前記指定により次候補に挙げられた身体的特徴を用いて認証するという段階的選定を前記複数種類の身体的特徴を全て使用するまで反復して行うことを特徴とする個人認証方法。

【請求項３】 個人固有の身体的特徴を抽出し該身体的特徴を用いて本人確認を行う個人認証方法において、利用者側端末が通信ネットワークを介してセンタ側装置に接続されており、前記センタ側装置あるいは利用者が複数種類の身体的特徴のなかから使用する身体的特徴を順に選定して認証に用い、かつ、認証に係る処理は前工程と後工程の２つに分割されている個人認証方法であって、

前記センタ側装置が身体的特徴の選定を行う場合には、複数種類の身体的特徴における認証結果をテーブルに記憶しておき、予め設定された個人認証のセキュリティレベルの情報と前記テーブルの情報とを用いて各身体的特徴の信頼性を表わす評価関数を計算することにより複数種類のなかから認証に最も適する身体的特徴と前工程の処理方法とを前記端末に送信し、前記端末は前記前工程処理により前記センタ側装置が指定した身体的情報を入力して身体的特徴の抽出を行い前記センタ側装置に送信し、前記センタ側装置では後工程処理により前記端末から送信された身体的特徴と予め登録している特定個人の身体的特徴とを照合し前記身体的特徴が前記特定個人のものか否かの判定を行い、前記特定個人と判定されたときは認証処理を終了し、前記特定個人と判定されなかったときは前記選定により次候補として挙げられた身体的特徴を用いて認証するという段階的選定を前記複数種類の身体的特徴を全て使用するまで反復して行い、

利用者が使用する身体的特徴の決定を行う場合には、前記利用者側端末は前記認証サーバから送信されてきた前工程処理方法により利用者の指定した身体的情報を入力して身体的特徴の抽出を行い前記センタ側装置に送信し、前記センタ側装置では後工程処理により前記端末から送信された身体的特徴と予め登録している特定個人の身体的特徴とを照合し前記身体的特徴が前記特定個人のものか否かの判定を行い、前記特定個人と判定されたときは認証処理を終了し、前記特定個人と判定されなかったときは前記指定により次候補に挙げられた身体的特徴を用いて認証するという段階的選定を前記複数種類の身体的特徴を全て使用するまで反復して行うことを特徴とする個人認証方法。

【請求項４】 前記センタ側装置と前記利用者側端末との間の通信は公開鍵暗号方式で行うものであることを特徴とする請求項２または請求項３記載の個人認証方法。

【請求項５】 前記テーブルは認証が行われる毎に得られる判定結果により内容が更新されることを特徴とする請求項１ないし請求項３のうちいずれか１項記載の個人認証方法。

【請求項６】 複数種類の身体的特徴のなかから１つの身体的特徴を使用して認証を行う処理をコンピュータに実行させる個人認証プログラムを記録した記録媒体であって、

認証結果をテーブルに記憶する手順と、個人認証のセキュリティレベルを設定する手順と、該セキュリティレベルの情報と前記テーブルの情報とを用いて各身体的特徴の信頼性を表わす評価関数を計算することにより前記複数種類の身体的特徴のなかから認証に最も適する身体的特徴を選定する手順と、利用者から得られた身体的特徴と予め登録している特定個人の身体的特徴とを照合し前記身体的特徴が前記特定個人のものか否かの判定を行い、前記特定個人と判定されたときは認証処理を終了し、前記特定個人と判定されなかったときは前記評価関数により次候補として挙げられた身体的特徴を用いて認証するという段階的選定を複数種類の身体的特徴を全て使用するまで反復して行う手順とを有することを特徴とする個人認証プログラムを記録した記録媒体。

【請求項7】 前記テーブルは認証が行われる毎に得られる判定結果により内容が更新されることを特徴とする請求項6記載の個人認証プログラムを記録した記録媒体。

【請求項8】 利用者側端末が通信ネットワークを介してセンタ側装置に接続されており、前記センタ側装置あるいは利用者が複数種類の身体的特徴のなかから使用する身体的特徴を順に選定して認証を行う前記センタ側装置の処理を実行する個人認証プログラムを記録した記録媒体であって、

複数種類の身体的特徴における認証結果をテーブルに記憶する手順と、個人認証のセキュリティレベルを設定する手順と、該セキュリティレベルの情報と前記テーブルの情報とを用いて各身体的特徴の信頼性を表わす評価関数を計算することにより複数種類の身体的特徴のなかから認証に最も適する身体的特徴を選択する手順と、前記利用者側端末から送信された身体的特徴と予め登録している特定個人の身体的特徴とを照合し前記身体的特徴が前記特定個人のものか否かの判定を行い、前記特定個人と判定されたときは認証処理を終了し、前記特定個人と判定されなかったときは前記選択により次候補として挙げられた身体的特徴を用いて認証するという段階的選定を前記複数種類の身体的特徴を全て使用するまで反復して行う手順とを有することを特徴とする個人認証プログラムを記録した記録媒体。

【請求項9】 利用者側端末が通信ネットワークを介してセンタ側装置に接続されており、前記センタ側装置あるいは利用者が複数種類の身体的特徴のなかから使用する身体的特徴を順に選定して認証を行う前記利用者側端末の処理を実行する個人認証プログラムを記録した記録媒体であって、

利用者自ら個人認証のセキュリティレベルを設定する手順と、指定した身体的情報を入力して身体的特徴の抽出を行い前記センタ側装置に送信する手順と、前記センタ側装置において本人と認証されなかったときは前記指定により次候補に挙げられた身体的特徴を用いて認証するという段階的選定を前記複数種類の身体的特徴を全て使用するまで反復して行う手順を有することを特徴とする個人認証プログラムを記録した記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、個人認証方法およびその装置、特に複数の身体的特徴を用いて認証を行う方法およびその装置に関する。

【0002】

【従来の技術】通信ネットワークを介したサービスにおけるセキュリティ確保の手段としてパスワードが常用されている。しかし、パスワードは盗用されると他人が本人になりすますことができる。これを防止するため、本人でしか有しえない指紋・筆跡等の身体的特徴（バイオメトリクス）を用いる方法がある。しかしこれも、周囲環境の変化により常に安定に認証されるとは限らない。また、模擬・模造される危険性もあるといった問題が内在する。このため複数のバイオメトリクスを用いる方法が考えられている。

【0003】

【発明が解決しようとする課題】複数バイオメトリクスの使用法は次の2種類に大別される。その第一は、認証手段の二重化であり、特開平10-137222 にみられるように2種類のバイオメトリクスの一方で認証できない場合はもう一方で認証するという方法を採ることにより、本人であるにも拘わらず拒否されることへの回避を図っている。第二は、認証精度の向上であり、特開平08-16788、特開平10-137221 にみられるような複数バイオメトリクスの認証結果の重み付き結合がよく採られている。しかし、第一の方法は本人受理を容易化したものの他人拒否の機能は低下しており、第二の方法は重みは固定となっているので装置を設計したときと異なる要求が発生したときあるいは使用環境が変化したとき、重みが調整できないという問題がある。

【0004】以上述べたように従来の方法では、本人受理と他人拒否の重視度が用途によって異なるなかで複数バイオメトリクスを如何に使用するかという方式が確立されていない問題点があった。また、多種多様な用途に応じた認証サーバを構築するには個別のカスタマイズが、さらに環境の変化に応じるためにはきめ細かなチューニングが必要となり、手数がかかるという問題点があった。本発明は前記問題点を解決するためになされたものであり、その目的とするところは本人受理・他人拒否の両要求を満足する個人認証方法及びその装置を提供し、また、実際の使用環境に追随して適応していく個人認証方法及びその装置を提供するところにある。

【0005】

【課題を解決するための手段】上記の目的を達成するために、本発明は次のように構成することができる。本発明は、個人固有の身体的特徴を抽出し該身体的特徴を用

いて本人確認を行う個人認証方法であり、複数種類の身体的特徴における認証結果をテーブルに記憶しておき、予め設定された個人認証のセキュリティレベルの情報と前記テーブルの情報とを用いて各身体的特徴の信頼性を表わす評価関数を計算することにより前記複数種類の身体的特徴のなかから認証に最も適する身体的特徴を選定して利用者に該身体的特徴の入力を要求し、利用者から得られた身体的特徴と予め登録している特定個人の身体的特徴とを照合し前記身体的特徴が前記特定個人のものか否かの判定を行い、前記特定個人と判定されたときは認証処理を終了し、前記特定個人と判定されなかったときは前記評価関数により次候補として挙げられた身体的特徴を用いて認証するという段階的選定を複数種類の身体的特徴を全て使用するまで反復して行う。

【０００６】本発明によれば、最適な身体的特徴を選定することが可能であり、例えば、特開平１１－５３５４０にあるようにランダムに身体的特徴を選定する方法よりも確実に認証を行うことが可能となる。本発明は次のように構成することもできる。本発明は、個人固有の身体的特徴を抽出し該身体的特徴を用いて本人確認を行う個人認証方法において、利用者側端末が通信ネットワークを介してセンタ側装置に接続されており、前記センタ側装置あるいは利用者が複数種類の身体的特徴のなかから使用する身体的特徴を順に選定して認証に用いる方法であり、センタ側装置が身体的特徴の選定を行う場合には、複数種類の身体的特徴における認証結果をテーブルに記憶しておき、予め設定された個人認証のセキュリティレベルの情報と前記テーブルの情報とを用いて各身体的特徴の信頼性を表わす評価関数を計算することにより複数種類の身体的特徴のなかから認証に最も適する身体的特徴を選択して該身体的特徴の名称を前記利用者側端末に送信し、利用者は前記センタ側装置が指定した身体的情報を入力して身体的特徴の抽出を行い前記センタ側装置に送信し、前記センタ側装置では前記利用者側端末から送信された身体的特徴と予め登録している特定個人の身体的特徴とを照合し前記身体的特徴が前記特定個人のものか否かの判定を行い、前記特定個人と判定されたときは認証処理を終了し、前記特定個人と判定されなかったときは前記選択により次候補として挙げられた身体的特徴を用いて認証するという段階的選定を前記複数種類の身体的特徴を全て使用するまで反復して行い、利用者が身体的特徴の選定を行う場合には、利用者は自ら指定した身体的情報を入力して身体的特徴の抽出を行い前記センタ側装置に送信し、前記センタ側装置では前記利用者側端末から送信された身体的特徴と予め登録している特定個人の身体的特徴とを照合し前記身体的特徴が前記特定個人のものか否かの判定を行い、前記特定個人と判定されたときは認証処理を終了し、前記特定個人と判定されなかったときは前記指定により次候補に挙げられた身体的特徴を用いて認証するという段階的選定を前記複数種類の身体的特徴を全て使用するまで反復して行う。

【０００７】更に、本発明は次のように構成することもできる。本発明は、個人固有の身体的特徴を抽出し該身体的特徴を用いて本人確認を行う個人認証方法において、利用者側端末が通信ネットワークを介してセンタ側装置に接続されており、前記センタ側装置あるいは利用者が複数種類の身体的特徴のなかから使用する身体的特徴を順に選定して認証に用い、かつ、認証に係る処理は前工程と後工程の２つに分割されている個人認証方法であり、前記センタ側装置が身体的特徴の選定を行う場合には、複数種類の身体的特徴における認証結果をテーブルに記憶しておき、予め設定された個人認証のセキュリティレベルの情報と前記テーブルの情報とを用いて各身体的特徴の信頼性を表わす評価関数を計算することにより複数種類のなかから認証に最も適する身体的特徴と前工程の処理方法とを前記端末に送信し、前記端末は前記前工程処理により前記センタ側装置が指定した身体的情報を入力して身体的特徴の抽出を行い前記センタ側装置に送信し、前記センタ側装置では後工程処理により前記端末から送信された身体的特徴と予め登録している特定個人の身体的特徴とを照合し前記身体的特徴が前記特定個人のものか否かの判定を行い、前記特定個人と判定されたときは認証処理を終了し、前記特定個人と判定されなかったときは前記選定により次候補として挙げられた身体的特徴を用いて認証するという段階的選定を前記複数種類の身体的特徴を全て使用するまで反復して行い、利用者が使用する身体的特徴の決定を行う場合には、前記利用者側端末は前記認証サーバから送信されてきた前工程処理方法により利用者の指定した身体的情報を入力して身体的特徴の抽出を行い前記センタ側装置に送信し、前記センタ側装置では後工程処理により前記端末から送信された身体的特徴と予め登録している特定個人の身体的特徴とを照合し前記身体的特徴が前記特定個人のものか否かの判定を行い、前記特定個人と判定されたときは認証処理を終了し、前記特定個人と判定されなかったときは前記指定により次候補に挙げられた身体的特徴を用いて認証するという段階的選定を前記複数種類の身体的特徴を全て使用するまで反復して行う。

【０００８】これらの発明によっても、最適な身体的特徴を選定することが可能となり、例えば、特開平１１－５３５４０にあるようにランダムに身体的特徴を選定する方法よりも確実に認証を行うことが可能となる。更に、ユーザが適切な身体的特徴を選択することもできるので、更に利便性が向上する。上記の構成において、前記センタ側装置と前記利用者側端末との間の通信は公開鍵暗号方式で行うようにすることができる。

【０００９】また、前記テーブルは認証が行われる毎に得られる判定結果により内容が更新されることとしてもよい。これによれば、指定した優先度を保持しつつ、経

時変化を伴う環境下でも最適な身体的特徴の選定が可能となる。本発明は、下記のような記録媒体として構成することもできる。すなわち、本発明は、複数種類の身体的特徴のなかから１つの身体的特徴を使用して認証を行う処理をコンピュータに実行させる個人認証プログラムを記録した記録媒体であって、認証結果をテーブルに記憶する手順と、個人認証のセキュリティレベルを設定する手順と、該セキュリティレベルの情報と前記テーブルの情報とを用いて各身体的特徴の信頼性を表わす評価関数を計算することにより前記複数種類の身体的特徴のなかから認証に最も適する身体的特徴を選定する手順と、利用者から得られた身体的特徴と予め登録している特定個人の身体的特徴とを照合し前記身体的特徴が前記特定個人のものか否かの判定を行い、前記特定個人と判定されたときは認証処理を終了し、前記特定個人と判定されなかったときは前記評価関数により次候補として挙げられた身体的特徴を用いて認証するという段階的選定を複数種類の身体的特徴を全て使用するまで反復して行う手順とを有する。

【００１０】また、本発明は次のように構成することもできる。本発明は、利用者側端末が通信ネットワークを介してセンタ側装置に接続されており、前記センタ側装置あるいは利用者が複数種類の身体的特徴のなかから使用する身体的特徴を順に選定して認証を行う前記センタ側装置の処理を実行する個人認証プログラムを記録した記録媒体であって、複数種類の身体的特徴における認証結果をテーブルに記憶する手順と、個人認証のセキュリティレベルを設定する手順と、該セキュリティレベルの情報と前記テーブルの情報とを用いて各身体的特徴の信頼性を表わす評価関数を計算することにより複数種類の身体的特徴のなかから認証に最も適する身体的特徴を選択する手順と、前記利用者側端末から送信された身体的特徴と予め登録している特定個人の身体的特徴とを照合し前記身体的特徴が前記特定個人のものか否かの判定を行い、前記特定個人と判定されたときは認証処理を終了し、前記特定個人と判定されなかったときは前記選択により次候補として挙げられた身体的特徴を用いて認証するという段階的選定を前記複数種類の身体的特徴を全て使用するまで反復して行う手順とを有する。

【００１１】更に、本発明は次のように構成することもできる。本発明は、利用者側端末が通信ネットワークを介してセンタ側装置に接続されており、前記センタ側装置あるいは利用者が複数種類の身体的特徴のなかから使用する身体的特徴を順に選定して認証を行う前記利用者側端末の処理を実行する個人認証プログラムを記録した記録媒体であって、利用者自ら個人認証のセキュリティレベルを設定する手順と、指定した身体的情報を入力して身体的特徴の抽出を行い前記センタ側装置に送信する手順と、前記センタ側装置において本人と認証されなかったときは前記指定により次候補に挙げられた身体的特徴を用いて認証するという段階的選定を前記複数種類の身体的特徴を全て使用するまで反復して行う手順を有する。

【００１２】上記の記録媒体に記録されたプログラムをコンピュータに読み込ませることによって、本発明の個人認証方法を実施するためのセンタ側装置や利用者側端末を実現することが可能となる。上述したように、本発明は、本人受理・他人拒否の優先度をユーザ側あるいは認証サーバ側で設定を行い、該設定によりサーバを運用していく過程において使用したバイオメトリクスの認証結果を統計的情報としてテーブルに登録しておき認証が行われる毎に該テーブルを更新することにより最適なバイオメトリクスを使用できるようにしたものであり、認証サーバのカスタマイズ、チューニングの自動化が可能となる。

【００１３】

【発明の実施の形態】次に、本発明の実施例について図面を参照して説明する。図１は本発明の一実施例を示す個人認証システムのブロック構成図であって、ユーザ１、ユーザ端末２、通信ネットワーク３、認証サーバ４からなる。なお、認証サーバはセンタ側装置と称することもできる。ユーザ端末２は入力部２１、前工程処理部２２、表示部２３、使用順序メモリ部２４からなり、前工程処理部２２はN個の異なるセンサ（センサ１（２２１）、センサ２（２２２）、...、センサN（２２３））とこれに対応する特徴抽出部（特徴抽出部１（２２４）、特徴抽出部２（２２５）、...、特徴抽出部N（２２６））の組からなる。認証サーバ４は優先度設定部４１、判定結果格納テーブル１２、選択部４３、後工程処理部４１、個人特徴メモリ部４５からなる。後工程処理部４１はN個の照合部（照合部１（４４１）、照合部２（４４２）、...、照合部N（４４３））とこれに対応する判定部（判定部１（４４４）、判定部２（４４５）、...、判定部N（４４６））の組からなる。

【００１４】この個人認証システムは、ユーザ端末２において、複数のセンサのうちの１つのセンサにより取得した情報からそのセンサに対応する特徴抽出部により身体的特徴を取得し、認証サーバ４においてその身体的特徴を、登録してある特徴と照合して個人認証を行う。本実施例の動作を図２の処理フローを用いて説明する。図２のフローでは、特に、複数のバイオメトリクスから使用するバイオメトリクスを選択して使用する処理に着目している。

【００１５】複数のバイオメトリクスの中から如何なるバイオメトリクスを用いるかの選択権は認証サーバ１あるいはユーザ１の何れが有するかはステップ５０１において選択することができる。これは、例えば、ユーザが選択することができる。認証サーバ４に選択権がある場合、バイオメトリクスの使用順序k（k=1,2,...,N）は認証サーバ４が設定する。k=1 がセットされると（ステ

ップ５０２）、認証サーバ４は第k バイオメトリクスの情報を入力するよう通信ネットワーク３を介して表示部２３に提示する。ユーザ１は表示部２３の提示に従って第k バイオメトリクスの情報をN個の中の指定されたセンサから入力する。ユーザ端末２は抽出した特徴を通信ネットワーク３を介して認証サーバ４に送信し、認証サーバ４は後工程処理部４４で認証を行う（ステップ５０３）。ユーザ１が本人と判定されると（ステップ５０４）、受理を意味するメッセージが表示部２３に映し出され（ステップ５０５）、処理は終了する。

【００１６】本人と判定されないと（ステップ５０４）、k はk=k+1 にセットされ（ステップ５０６）、k 回までに使用されなかったバイオメトリクスのなかから次に指定されたバイオメトリクスを用いて認証が行われ（ステップ５０３）、本人か否かの判定がなされる（ステップ５０４）。前記処理が繰り返され、指定したN 個のバイオメトリクスを全て使用しても（k>N ）なお本人であると認証されない場合は（ステップ５０７）、最初から再試行となる（ステップ５０８）。

【００１７】ユーザ１に選択権がある場合は、ユーザ１はバイオメトリクスの使用順序k を入力部２１から設定する（ステップ５０９）。ユーザ端末２はk=1 にセットし（ステップ５１０）、第k バイオメトリクスを用いた認証が行われる（ステップ５１１）。ユーザ１が本人と判定されると（ステップ５１２）、受理され（ステップ５１３）、処理は終了する。本人と判定されない場合は（ステップ５１２）、k はk=k+1 に更新され（ステップ５１４）、使用バイオメトリクスを変えて認証が繰り返される。指定したN 個のバイオメトリクスを全て使用しても（k>N ）なお本人であると認証されない場合は（ステップ５１５）、最初から再試行となる（ステップ５１６）。

【００１８】次に、本実施例の詳細な動作を図３、図４を用いて説明する。図３は認証サーバ４に選択権がある場合の処理フローを示す図である。ユーザ１が入力部２１からＩＤ番号を投入すると認証サーバ４に送信される（ステップ１、２）。バイオメトリクスは認証精度の高いものから低いもの、ユーザにとって親和性のあるものから使いづらいものまで広範囲に存在する。優先度設定部４１、判定結果格納テーブル部４２、選択部４３における処理でバイオメトリクスが選択される。ここでは概要を説明し、詳細を後述する。

【００１９】優先度設定部４１は前記状況およびサービスの要求するセキュリティレベルを勘案し、本人受理、他人拒否の各要素の占める度合いを決定する（ステップ３）。選択部４３は本人受理、他人拒否の重視の度合いとユーザ１のこれまでの各バイオメトリクスによる認証結果が格納されている判定結果格納テーブル部４２の内容からN 個あるバイオメトリクスの中から１番目に使用する第１バイオメトリクスを後述する方法で決定し（ステップ４、５）、その名称をユーザ端末２に送信し表示部２３に表示する（ステップ６）。

【００２０】ユーザ１は前記表示を見て第１バイオメトリクスに対応するセンサを用いてバイオメトリクス情報を入力し（ステップ７）、前工程処理部２２に存在するプログラムを実行して特徴を抽出し（ステップ８）、認証サーバ４に送信する。認証サーバ４ではその特徴を受信し（ステップ９）、第１バイオメトリクスに対応する照合部のプログラムを起動して個人特徴メモリ部４５に格納されているユーザ１の登録特徴と送信されてきた第１バイオメトリクスの特徴との間で照合を行い類似度あるいは相違度等の尺度を得る（ステップ１０）。判定部では前記尺度に閾値を適用し前記第１バイオメトリクスの特徴が本人のものであるか否かの判定を行いその判定結果を判定結果格納テーブル部４２に書き込み、その内容を更新する。該判定結果が本人であった場合はユーザ端末２へのログインが受理され（ステップ１１、１２）、他人であった場合は拒否される（ステップ１３）。拒否が生じると選択部４３は残りの（N －１）個のバイオメトリクスの中から２番目に使用する第２バイオメトリクスを決定しその名称をユーザ端末２に送信し、上述した処理により第２バイオメトリクスによる認証が行われる（ステップ１４～）。以下、本人が認証されるまで前記処理が繰り返し行われ、全てのバイオメトリクスを使用しても本人認証に至らなかったときは、最初から再試行となる。

【００２１】図４はユーザ１に選択権がある場合の処理である。ユーザ１はＩＤ番号を投入し（ステップ１）、次いで、効率性・親和性等の観点から使い勝手がよく高精度で本人受理が可能となるバイオメトリクスを順に指定するとその内容は使用順序メモリ部２４に格納される（ステップ２、３）。続いて、使用順序メモリ部２４の内容が読出され第１バイオメトリクスの入力を促す旨のメッセージが表示部２３に表れるとユーザ１は第１バイオメトリクスに対応するセンサを用いてバイオメトリクス情報を入力し前工程処理部２２に存在するプログラムを実行して特徴を抽出し、認証サーバ４に送信する（ステップ４、５）。

【００２２】以下、照合・判定が実行され本人の受理・拒否が行われるところまでは図３の処理に同じである。異なるのは拒否の場合の後処理であり、図３では認証サーバ４は２番目の使用が決定されたバイオメトリクス名をユーザ端末２に送信したのに対し、図４では本人拒否通知を送信するところである（ステップ９）。本人拒否通知を受信すると（ステップ１０）、ユーザ１は上述した処理と同様の処理で第２バイオメトリクスによる認証を行い、以下、本人が認証されるまで前記処理が繰り返し行われ（ステップ１１～）、全てのバイオメトリクスを使用しても本人認証に至らなかったときは、最初から再試行となる。

【００２３】次に、前述したバイオメトリクスの選択の処理について詳細に説明する。図５は判定結果格納テーブル４２の内容を示す図であり、各バイオメトリクスに対する使用回数Ｔと本人拒否回数Ｒ、他人受理回数Ａが格納されている。Ｔ、Ｒ、Ａは初期値は共に零である。あるバイオメトリクスによる認証が実行されると、そのバイオメトリクスに対応するＴは１だけインクリメントされ、認証の結果、ユーザ１と認証されなければＲは１だけインクリメントされる。他人受理回数Ａを実際の運用で測定することは難しいので、ユーザ１と認証されなかったとき、個人特徴メモリ部４５に格納されているユーザ１以外の全てのユーザの特徴を入力として後工程処理部４４でユーザ１の特徴との照合を行いユーザ１と認証されれば、他人受理が行われたものとしてＡは１だけインクリメントされる。このように、Ｔ、Ｒ、Ａは認証が実行される毎にその値が更新される。

$$G = 1 - (R + \alpha A) / T \quad (1)$$

の値を求める。式(1) の右辺第２項でＡはＲに比してα倍の重みがかけられている。式(1) の右辺第２項はペナルティの項であり、Ｇ の値はＡ、Ｒが小さいほど大きくなり、Ｒ= Ａ=0のとき最大値１をとる。最大値検出回路４３２は選考対象とするＧ の値の中における最大値を検出し、対応するバイオメトリクス名をユーザ端末２の表示部２３に表示し、ユーザ１にそのバイオメトリクス情報の入力を促す。Ｇ は認証の都度計算されるので、当初、高頻度で使用していたユーザ１のバイオメトリクスが時間経過とともに認証精度が下降してきた場合、認証サーバ４が代替となり得るバイオメトリクスを発見する。もし、多数のユーザの中にユーザ１のバイオメトリクスと類似のバイオメトリクスを有するユーザがいても認証サーバ４がそのバイオメトリクスと異なるものを使用するよう指示するので信頼性の高い認証が可能となる。類似のバイオメトリクスを有する新規ユーザが途中から参加した場合、やはり、認証サーバ４の誘導により異なるバイオメトリクスの使用に転換することができる。このように、使用環境が変化してもこれに追随できる仕組みとなっているので常に安定した認証が可能となる。また、上記操作は認証サーバ４が自動で行うので人手によるカスタマイズ、チューニングの負担はかからない。

【００２５】図３、図４は前工程処理、後工程処理のプログラムがそれぞれ前工程処理部２２、後工程処理部４４に据付けになっている場合の処理手順を示しているが、前工程処理のプログラムを認証サーバ４が送信することも可能であり、図７、図８はそのような構成における処理手順を示す図である。なお、以下の説明で用いられるProGUI等は各構成要素を示す記号であり、以下、記号のみでその要素を参照する場合がある。

【００２６】図７は認証サーバ４に選択権がある場合の処理である。ユーザ１はユーザの公開鍵Pk(A) 、秘密鍵Sk(A) を生成し、次いでPk(A) とＩＤ番号を認証サーバ４に送信する（ステップ１、２）。認証サーバ４はそれらを受信し（ステップ３）、優先度設定部４１、選択部４３を相次いで起動し（ステップ４、５）、第１バイオメトリクスB1を得る（ステップ６）。また、ユーザ端末２においてバイオメトリクス情報の入力メニューを表示するＧＵＩ制御プログラムProGUIを読み出す（ステップ７）。さらに、認証サーバ４は特徴抽出プログラムProFow、スクランブルプログラムSXPro をPk(A) で暗号化したEPk(A)(ProFow, SXPro) を作成し（ステップ８）、B1、ProGUI、EPk(A)(ProFow, SXPro) をユーザ端末２に送信する。ユーザ端末２ではProFow, SXPro が秘密鍵Sk(A) により解読され（ステップ９、１０）、ユーザ１はProGUIの指示に従ってB1に対応するセンサから入力し（ステップ１１）、ProFowを実行して特徴Kaz を抽出する（ステップ１２）。次に、SXPro によりKaz にスクランブルを掛けてKaz (-1) を得（ステップ１３）、これらにESk(A)により暗号化したESk(A)(Kaz (-1) , ID) を認証サーバ４に送信する（ステップ１４）。

【００２７】認証サーバ４ではPk(A) により解読を行い（ステップ１５、１６）、Kaz (-1) を取り出す。そして、個人特徴メモリ部４５からスクランブルの掛けられたユーザ１の特徴Kaz(0) (-1) が読み出され（ステップ１７）、スクランブル解読プログラムSXPro (-1) によりKaz 、Kaz(0)が復元される（ステップ１８）。この後、照合部、判定部を起動してKaz の認証を行う一連の処理シーケンスは図３に同じである。

【００２８】図８はユーザ１に選択権がある場合の処理である。ユーザ１は効率性・親和性等の観点から使い勝手がよく高精度で本人受理が可能となるバイオメトリクスを順に指定し、使用順序メモリ部２４に格納しておく。ユーザ１がユーザの公開鍵Pk(A) 、ＩＤ番号、および、使用順序メモリ部２４から読出したB1を認証サーバ４に送信し（ステップ１～３）、認証サーバ４から返信されてきたB1の特徴抽出プログラムProFowを用いて特徴Kaz を抽出し（ステップ４～９）、スクランブルプログラムSXPro によりスクランブルをかけたデータと使用順序メモリ部２４から読出した第１バイオメトリクス名B1とを認証サーバ４に送信する（ステップ１０、１１）。

【００２９】この後、照合・判定が実行され本人の受理・拒否が行われるところは図７の処理に同じである。異なるのは拒否の場合の後処理であり、図７では認証サーバ４はB2およびB2の特徴を抽出するためのプログラムPr

aGUI、ProFowとスクランブルプログラムSXProをユーザ端末２に送信したのに対し、図８ではB2が不要である。前記データを受信すると、ユーザ１は上述した処理と同様の処理でB2による認証を行い、以下、本人が認証されるまで前記処理が繰り返し行われ、全てのバイオメトリクスを使用しても本人認証に至らなかったときは、最初から再試行となる。

【００３０】なお、上記のように、個人認証処理における工程を分け、端末とサーバでそれぞれの処理を行うこととすることにより、セキュリティーを保ち、通信量を削減することができる。また、プログラムを暗号化して端末に送ることにより、アルゴリズムの変更等を容易に行うことができ、更にセキュリティーを高めることが可能となる。

【００３１】本発明の個人認証システムは図１に示した構成に限定されず、種々の構成が可能である。例えば、図９に示した構成とすることができる。この個人認証システムは、ユーザ１、ユーザ端末２、通信ネットワーク３、認証サーバ４から構成される。図１では照合部（照合部１（４４１）、照合部２（４４２）、...、照合部N（４４３））が認証サーバ４にあるのに比べ、図９ではユーザ端末２に配置されているところが異なる。

【００３２】この例においても、複数のバイオメトリクスの中から如何なるバイオメトリクスを用いるかの選択権は認証サーバ４あるいはユーザ１の何れが有してもよい。認証サーバ４に選択権がある場合は、バイオメトリクスの使用順序k （k=1,2,...,K、K ；使用するバイオメトリクスの種類数）は認証サーバ４が設定する。k=1がセットされると認証サーバ４は第k バイオメトリクスの情報を入力するよう通信ネットワーク３を介して表示部２３に提示する。ユーザ１は第k バイオメトリクスの情報をN個の中の指定されたセンサから入力し抽出した特徴を用いて照合を行い、その結果を通信ネットワーク３を介して認証サーバ４に送信し、認証サーバ４は判定部で本人か否かの判定を行う。ユーザ１が本人と判定されると受理を意味するメッセージが表示部２３に映し出され処理は終了する。本人と判定されないと、k はk=k+1 にセットされ、次に指定されたバイオメトリクスを用いて前記手順で認証が行われ本人か否かの判定がなされる。前記処理が繰り返され、指定したN 個のバイオメトリクスを全て使用してもなお本人であると認証されない場合は最初から再試行となる。

【００３３】ユーザ１に選択権がある場合は、ユーザ１はバイオメトリクスの使用順序k を入力部２１により設定し、使用順序メモリ部２４に格納される。ユーザ端末２はk=1 にセットし、第k バイオメトリクスを用いた認証が行われる。ユーザ１が本人と判定されると受理され処理は終了する。本人と判定されない場合はk はk=k+1 に更新され、使用順序メモリ部２４に格納された情報が読出され使用バイオメトリクスを変えて認証が繰り返される。指定したN 個のバイオメトリクスを全て使用してもなお本人であると認証されない場合は最初から再試行となる。

【００３４】本実施例の図９では照合部（照合部１（４４１）、照合部２（４４２）、...、照合部N（４４３））がユーザ端末２にある例を述べたが、判定部（判定部１（４４４）、判定部２（４４５）、...、判定部N（４４６））までもがユーザ端末２に属し、判定結果のみが認証サーバ４に送信される構成であっても良い。更に、特徴入力から判定及びバイオメトリクス選択をスタンドアロンで実施する個人認証装置とすることも可能である。

【００３５】上述した各構成要素を実現するプログラムはCD－ROMやフロッピー（登録商標）ディスク等の記録媒体に格納することができる。記録媒体に格納されたプログラムをコンピュータにインストールすることにより本発明の端末や認証サーバの処理を行うことが可能である。また、上記のプログラムをコンピュータにプレインストールしておくことも可能である。

【００３６】以上、本発明を実施例に基づき具体的に説明したが、本発明は前記実施例に限定されるものではなく、その主旨を逸脱しない範囲において種々変更可能であることは言うまでもない。

【００３７】

【発明の効果】以上説明したように本発明によれば、本人受理・他人拒否の優先度設定をユーザ側あるいは認証サーバ側で行い、運用過程におけるバイオメトリクスの認証結果を統計的情報としてテーブルに登録しておき認証の都度更新するようにしたため、指定した優先度を保持しつつ最適なバイオメトリクスを使用できる長所がある。また、更新は自動で行われる仕組みになっているため、多種多様な用途に供するための労力の削減、経時変化を伴う環境下への適用が可能になるという長所がある。

【図面の簡単な説明】

【図１】本発明の一実施例を示す個人認証システムのブロック構成図である。

【図２】図１における個人認証システムの処理フロー図である。

【図３】図１における個人認証システムで認証サーバ４に選択権がある場合の通信制御フロー図である。

【図４】図１における個人認証システムでユーザ１に選択権がある場合の通信制御フロー図である。

【図５】判定結果格納テーブル４２の一例を示す図である。

【図６】選択部４３のブロック構成図である。

【図７】図１の個人認証システムで認証サーバ４に選択権があるときに前工程処理のプログラムが認証サーバ４から送信されて来る場合の通信制御フロー図である。

【図８】図１における個人認証システムでユーザ１に選

択権があるときに前工程処理のプログラムが認証サーバ１から送信されて来る場合の通信制御フロー図である。

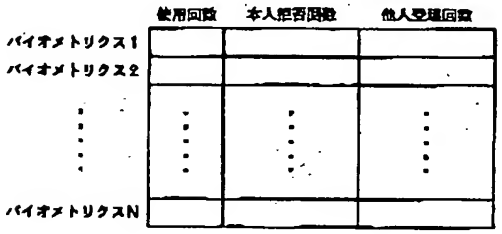
【図９】本発明の別の実施例を示す個人認証システムのブロック構成図である。

【符号の説明】

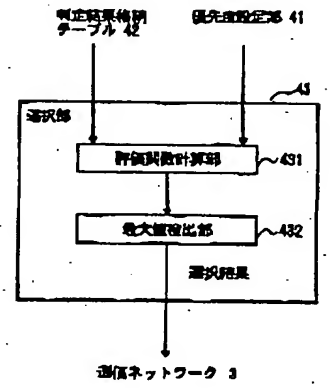
１　ユーザ
２　ユーザ端末
３　通信ネットワーク
４　認証サーバ
２１　入力部
２２　前工程処理部
２３　表示部
２２１　センサ１

２２２　センサ２
２２３　センサN
２２４　特徴抽出部１
２２５　特徴抽出部２
２２６　特徴抽出部N
４１　優先度設定部
４２　判定結果格納テーブル
４３　選択部
４４　後工程処理部
４５　個人特徴メモリ部
４４１　照合部１
４４２　照合部２
４４３　照合部N

【図５】

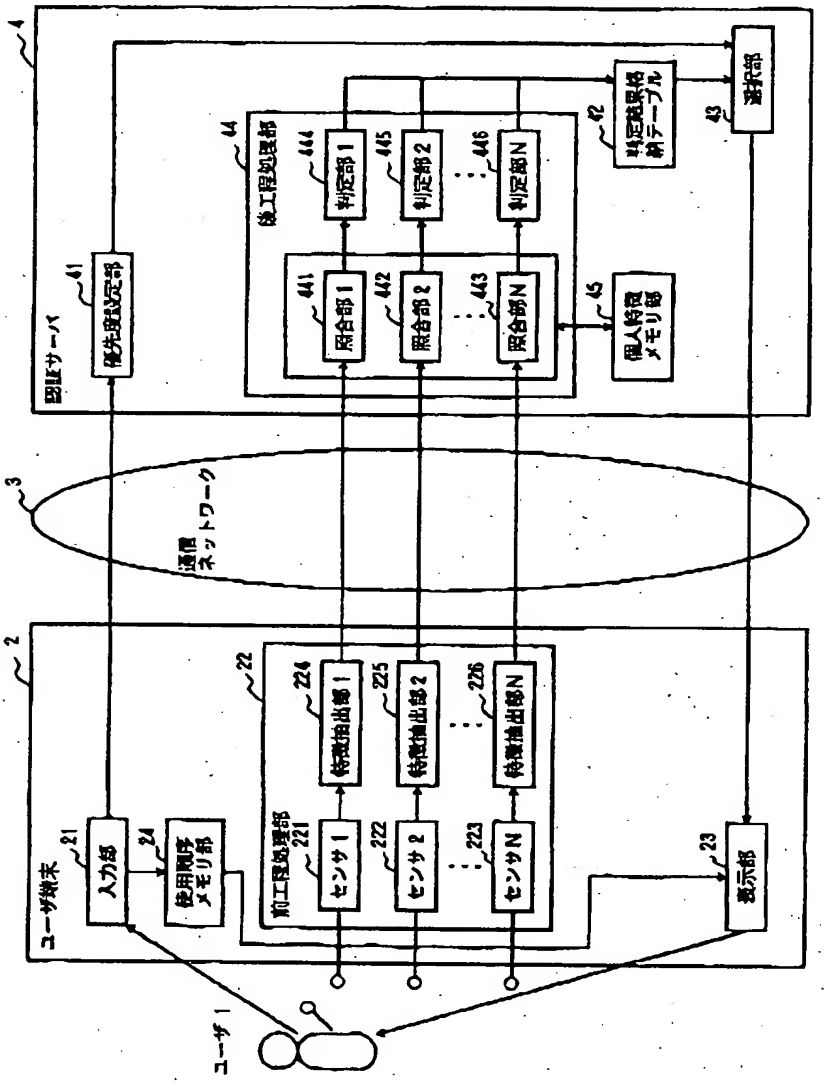


【図６】



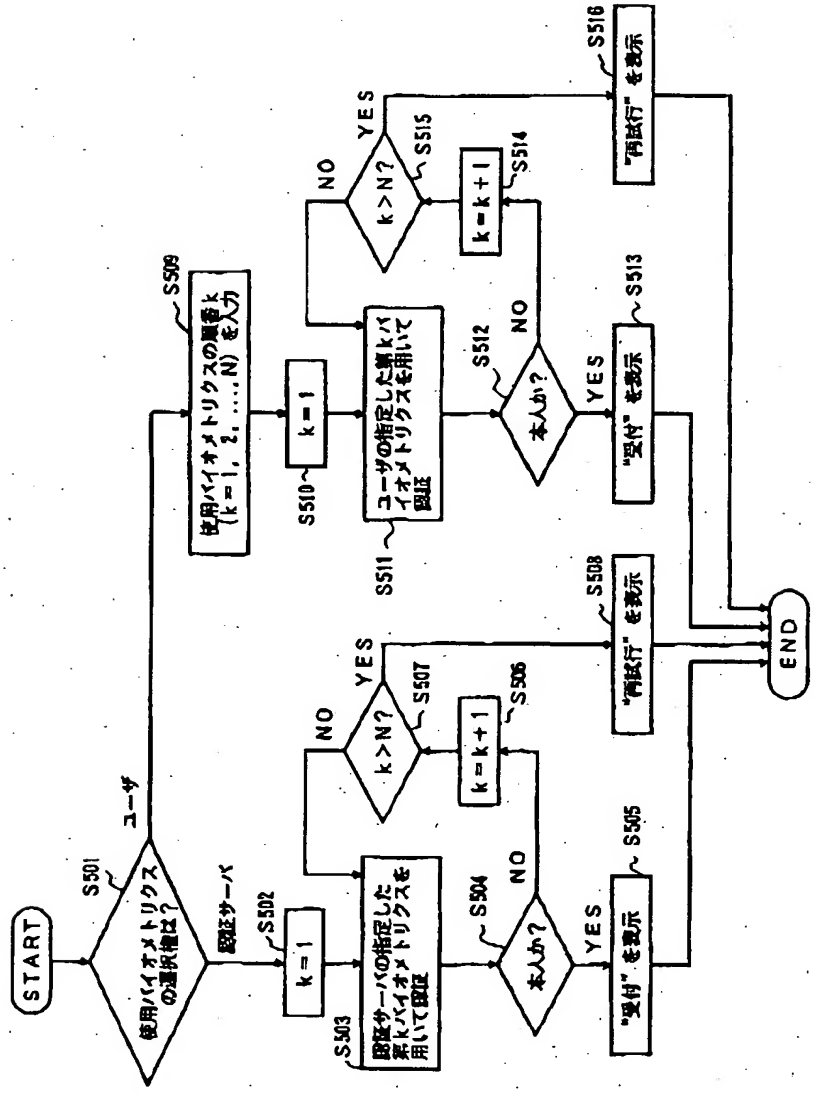
【図1】

本発明の一実施例を示す個人認証システムのブロック構成図



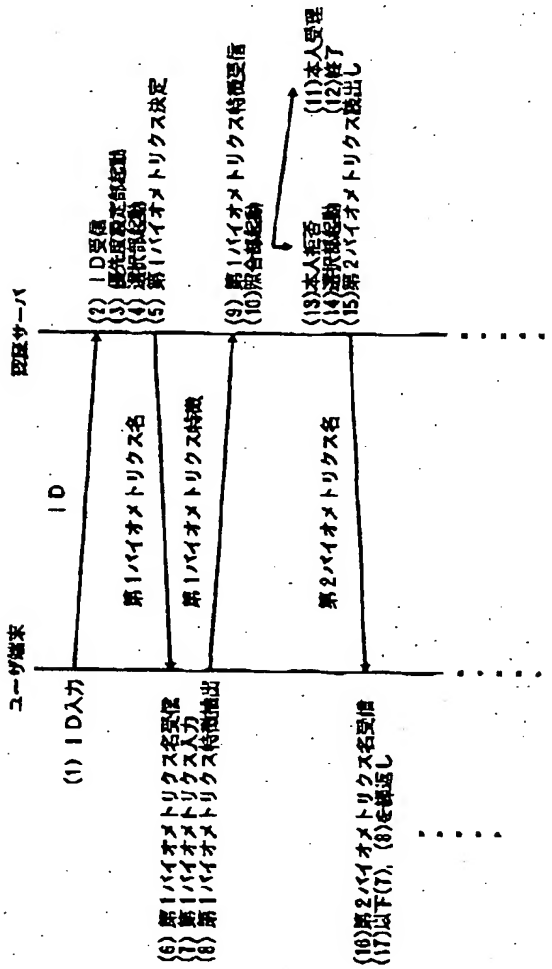
【図2】

図1における個人認証システムの処理フロー図



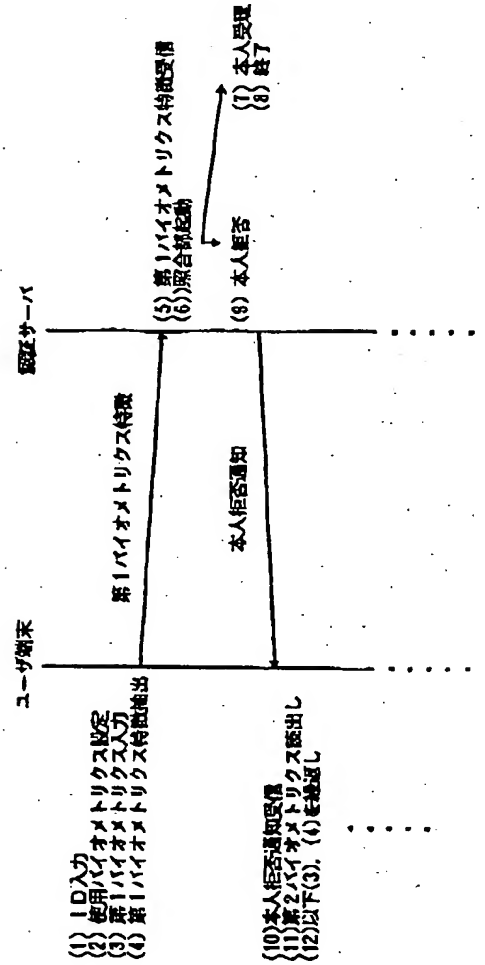
【図3】

図1における個人認証システムで認証サーバ4に選択権がある場合の通信制御フロー図



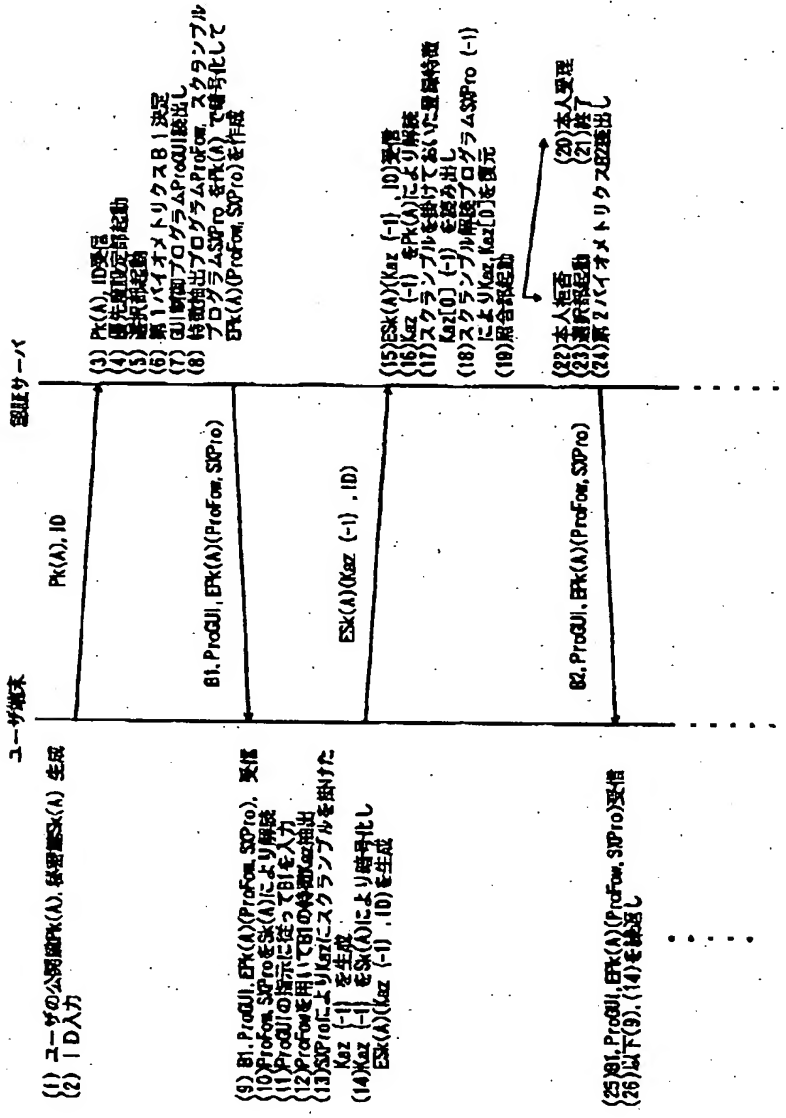
【図4】

図1における個人認証システムでユーザ1に選択権がある場合の通信制御フロー図



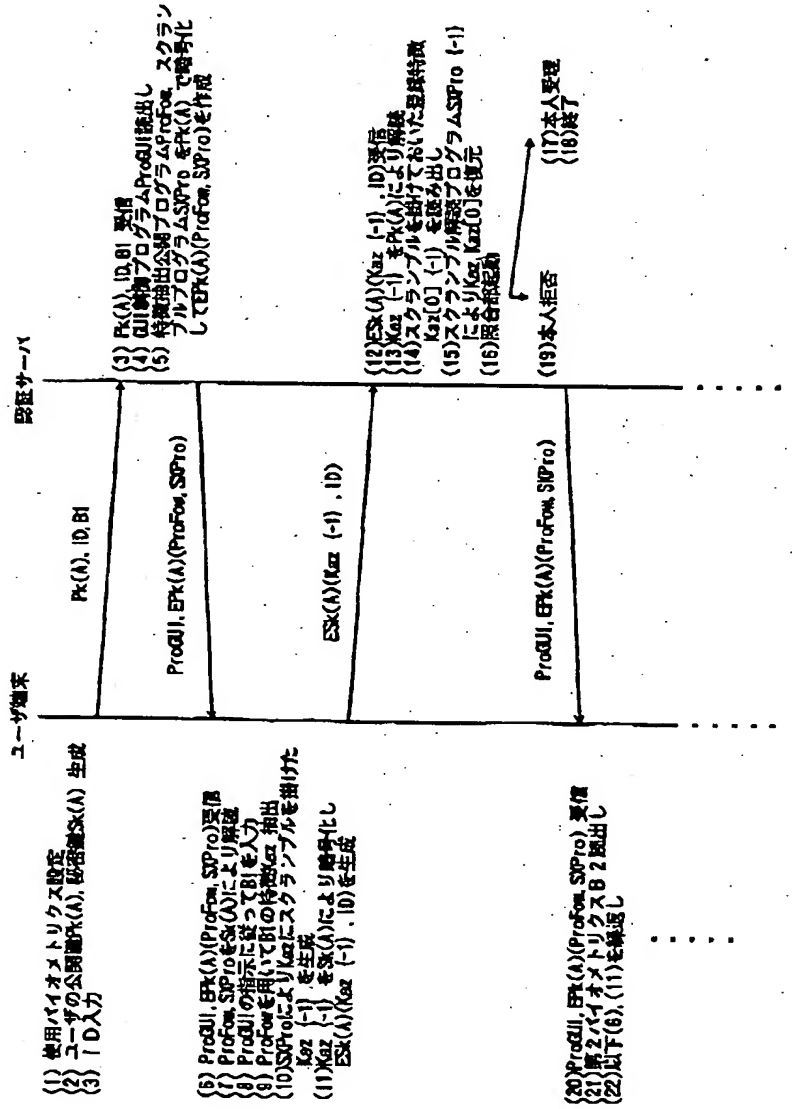
【図7】

図１の個人認証システムで認証サーバ４に選択権があるときに前工程処理のプログラムが認証サーバ４から送信されて来る場合の通信制御フロー図



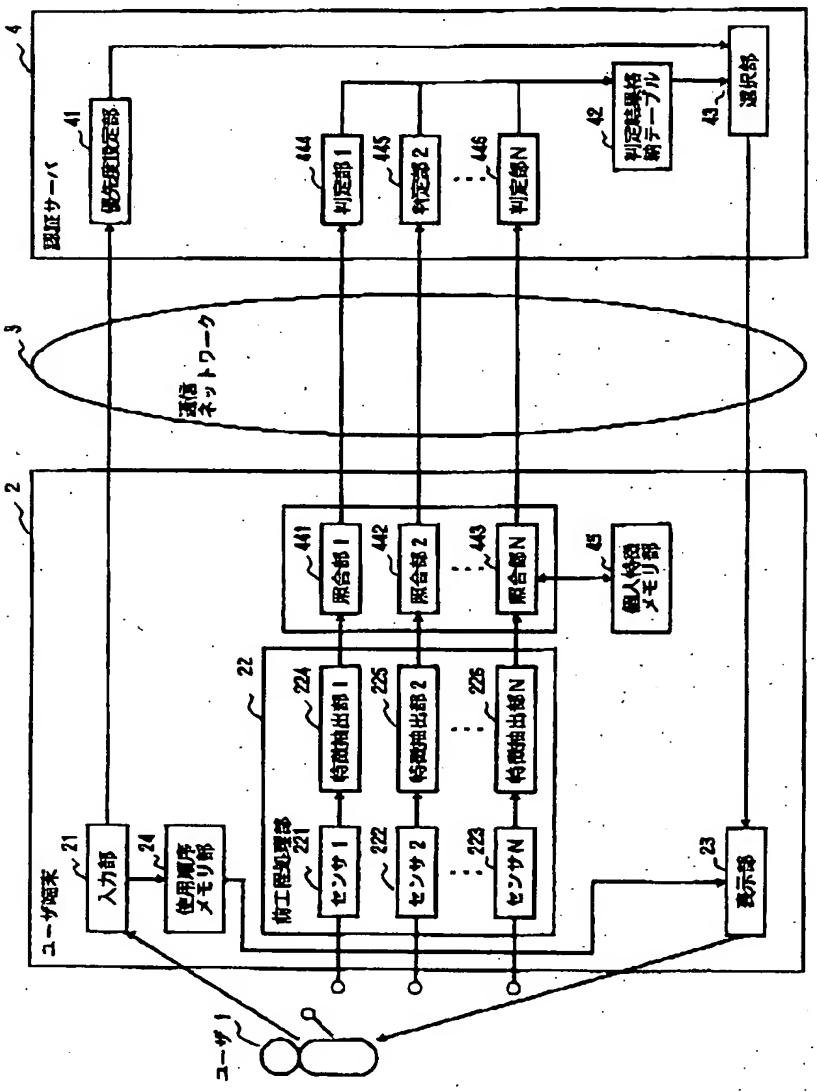
【図8】

図1における個人認証システムでユーザ1に選択権があるときに前工程処理のプログラムが認証サーバ4から送信されて来る場合の通信制御フロー図



【図9】

本発明の別の実施例を示す個人認証システムのブロック構成図



フロントページの続き

(72)発明者　若原　徹
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

(72)発明者　外波　雅史
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

(72)発明者 堀岡 力
東京都千代田区大手町二丁目3番1号 日本電信電話株式会社内
(72)発明者 田中 滑人
東京都千代田区大手町二丁目3番1号 日本電信電話株式会社内
(72)発明者 山中 喜義
東京都千代田区大手町二丁目3番1号 日本電信電話株式会社内
(72)発明者 小松 尚久
東京都国分寺市光町1－26－24

Fターム(参考) 5B043 AA09 BA02 BA06 CA09 FA02 FA08 GA13
5B085 AE25